Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та кібербезпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

КОМП'ЮТЕРНА МЕРЕЖА САЛОНУ КРАСИ НА ОСНОВІ ОБЛАДНАННЯ CISCO

BEAUTY SALON COMPUTER NETWORK BASED ON CISCO EQUIPMENT

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Хвень Діана Андріївна

(підпис)

Керівник:
д.пед.н., професор
Чернящук Наталія Леонідівна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 17 » червня 2024 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2024 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та кібербезпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ проф. Н.Чернящук
« 10 » 01 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Хвень Діані Андріївні
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Комп'ютерна мережа салону краси на основі обладнання Cisco*

Керівник роботи *д.пед.н., професор Чернящук Наталія Леонідівна*

затверджені наказом закладу вищої освіти від «30» грудня 2023 року № 459/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 11.06.2024р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Постановка задачі та огляд систем
Огляд технологій
Програмна реалізація та отримані результати
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Мережа VPN
Віртуалізація мережі
Протокол безпеки
Підтримка IPv4 та IPv6
Ipsec
Режими роботи IPsec

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз проблеми за темою роботи та постановка завдань дослідження	*Чернящук Н.Л., професор*		
Теоретичне дослідження та практична реалізація	*Чернящук Н.Л., професор*		
Практична реалізація об'єкта проектування	*Чернящук Н.Л., професор*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Лавренчук С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І.,асистент*		

7. Дата видачі завдання 10.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Розділ 1. Огляд літератури із досліджуваної проблеми. Теоретичні основи комп'ютерної мережі*	до 15.02.2024 р.	Виконано
2.	*Розділ 2. Реалізація комп'ютерної мережі*	до 15.03.2024 р.	Виконано
3.	*Розділ 3. Створення мережевого зв'язку та виконання експериментів*	до 04.05.2024 р.	Виконано
4.	*Висновки та пропозиції*	до 07.05.2025 р.	Виконано
5.	*Формування списку використаних джерел*	до 10.05.2024 р.	Виконано
6.	*Формування додатків*	до 15.05.2024 р.	Виконано
7.	*Оформлення ілюстративного матеріалу*	до 20.05.2024 р.	Виконано
8.	*Нормоконтроль*	до 01.06.2024 р.	Виконано
9.	*Інструментальна перевірка на академічний плагіат*	до 04.06.2024 р	Виконано
10.	*Представлення кваліфікаційної роботи бакалавра до захисту*	до 11.06.2024 р.	Виконано

Здобувач вищої освіти _____ (підпис) Хвень Д.А. (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ (підпис) Чернящук Н.Л. (прізвище, ініціали)

АНОТАЦІЯ

Хвень Д.А. Комп’ютерна мережа салону краси на основі обладнання Cisco. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп’ютерна інженерія» спеціальності 123 Комп’ютерна інженерія. Луцький національний технічний університет. Луцьк, 2024.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, трьох додатків.

Метою роботи є створення ефективної, надійної та безпечної мережевої інфраструктури, яка забезпечить оптимізацію бізнес-процесів, покращення якості обслуговування клієнтів, підвищення продуктивності працівників та підтримку масштабованості бізнесу.

Досягнення цих цілей допоможе салону краси підвищити рівень обслуговування клієнтів, оптимізувати внутрішні процеси та забезпечити стабільний розвиток бізнесу, використовуючи передові мережеві технології від Cisco.

Об’єктом дослідження є мережева інфраструктура салону краси, яка включає апаратне та програмне забезпечення, призначене для забезпечення зв’язку, безпеки, автоматизації та ефективності роботи салону.

Предметом дослідження є розробка, впровадження, налаштування та експлуатація мережевої інфраструктури салону краси з використанням обладнання та технологій Cisco.

Ключові слова: комп’ютерна мережа, VPN, Site-to-Site, протоколи безпеки Ipsec.

ANNOTATION

Hven D.A. Beauty salon computer network based on Cisco equipment. Manuscript.

Bachelor's qualification thesis of the OP "Computer Engineering" specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2024.

The qualification work consists of an introduction, three sections, conclusions, a list of used sources, and three appendices.

The purpose of the work is to study the construction and configuration of a computer network of a beauty salon.

The object of research is computer networks.

The subject of the study is the hardware and software implementation of a VPN for a beauty salon.

Tasks of the bachelor's qualification work:

– analysis of basic information about computer networks;

– posing the problem of ensuring the security of network traffic and networks;

– classify computer networks;

– characteristics and purpose of VPN implementations – Site-to-Site and remote access;

– creation of an experimental stand.

Keywords: computer network, VPN, Site-to-Site, Ipsec security protocols.

ЗМІСТ

ВСТУП

Впровадження комп’ютерної мережі дозволяє автоматизувати багато бізнес-процесів, таких як запис клієнтів, управління персоналом, облік матеріалів і фінансів. Це сприяє зменшенню часу на виконання рутинних завдань і підвищенню продуктивності працівників. Мережа забезпечує швидкий і зручний доступ до інформації для клієнтів, наприклад, через онлайн-бронювання, програми лояльності, тощо. Оскільки салони краси працюють з персональними даними клієнтів, важливо забезпечити їх захист від несанкціонованого доступу. Обладнання Cisco пропонує розширені засоби кібербезпеки для захисту даних. Обладнання Cisco відоме своєю високою надійністю і стабільністю, що мінімізує ризики простоїв і втрат даних. Обладнання Cisco підтримує сучасні технології, що дозволяє легко інтегрувати нові сервіси і рішення, такі як системи управління запасами, відеоспостереження тощо. Використання сучасних мережевих технологій допомагає салону залишатися конкурентоспроможним, надаючи більш якісні і зручні послуги для клієнтів. Автоматизація і оптимізація процесів дозволяють персоналу більше зосередитися на клієнтах, що покращує загальний рівень обслуговування.

Хоча початкові інвестиції в обладнання Cisco можуть бути високими, довгострокові вигоди від зниження експлуатаційних витрат, підвищення ефективності і безпеки можуть значно перевищити ці витрати. Обладнання Cisco пропонує розширену підтримку і обслуговування, що мінімізує витрати на технічне обслуговування та ремонт. В цілому, створення комп’ютерної мережі салону краси на основі обладнання Cisco є актуальною темою через її значний вплив на ефективність, безпеку, масштабованість і конкурентоспроможність бізнесу.

Метою роботи є створення ефективної, надійної та безпечної мережевої інфраструктури, яка забезпечить оптимізацію бізнес-процесів, покращення якості обслуговування клієнтів, підвищення продуктивності працівників та підтримку масштабованості бізнесу.

Завдання дослідження включають:

– розробка детального плану мережі, що включає вибір необхідного обладнання Cisco (маршрутизатори, комутатори, точки доступу тощо) – для забезпечення стабільного та швидкого з’єднання;

– встановлення та налаштування мережевого обладнання відповідно до проекту;

– використання сучасних технологій захисту від несанкціонованого доступу, вірусів та інших загроз, що включає міжмережеві екрани (firewalls), системи виявлення і запобігання вторгненням (IDS/IPS);

– налаштування систем резервного копіювання даних та планів аварійного відновлення для забезпечення безперервної роботи бізнесу;

– впровадження систем управління записами, управління персоналом та обліку матеріалів для зменшення ручної роботи і мінімізації людських помилок;

– забезпечення безшовної інтеграції з системами точок продажу (POS) для оптимізації фінансових транзакцій та управління інвентарем.

Досягнення цих цілей допоможе салону краси підвищити рівень обслуговування клієнтів, оптимізувати внутрішні процеси та забезпечити стабільний розвиток бізнесу, використовуючи передові мережеві технології від Cisco.

Об’єктом дослідження є мережева інфраструктура салону краси, яка включає апаратне та програмне забезпечення, призначене для забезпечення зв’язку, безпеки, автоматизації та ефективності роботи салону.

Предметом дослідження є розробка, впровадження, налаштування та експлуатація мережевої інфраструктури салону краси з використанням обладнання та технологій Cisco.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1 Безпека комп'ютерних мереж

Віртуальні приватні мережі (Virtual Private Networks або VPNs) – це технологія, що дозволяє створювати безпечне з'єднання між двома або більше пристроями через неприватну мережу, таку як Інтернет. Основні відомості про віртуальні приватні мережі включають. Зашифроване з'єднання. VPN використовує шифрування для захисту мережевого трафіку від прослуховування або зловмисного втручання. Це робить його ідеальним варіантом для забезпечення приватності та безпеки під час передачі конфіденційної інформації через ненадійні мережі, такі як Інтернет. Віддалений доступ. VPN дозволяє користувачам встановлювати з'єднання з віддаленими мережами або ресурсами через Інтернет, надаючи їм можливість працювати з віддаленими серверами, файлообміном, програмними додатками тощо, як будто вони знаходяться в тій же мережі, що і ці ресурси. Маскування IP-адреси. VPN приховує реальну IP-адресу користувача, замінюючи її на IP-адресу VPN-сервера. Це дозволяє зберігати приватність та анонімність користувача в Інтернеті, ускладнюючи відстеження його дій. Географічне обмеження. VPN може допомогти обходити географічні обмеження, дозволяючи отримувати доступ до вмісту, який може бути недоступним у певних регіонах через обмеження або цензуру. Задача забезпечення безпеки мережевого трафіку та мереж в VPN включає в себе ряд заходів. Шифрування даних. Всі дані, що передаються через VPN, повинні бути шифровані, щоб унеможливити прослуховування або зловмисне втручання. Аутентифікація користувачів і пристроїв. Для забезпечення безпеки мережі важливо встановити ідентифікацію користувачів та пристроїв, які підключаються до VPN.

Управління доступом. VPN повинен мати механізми управління доступом, щоб контролювати, які користувачі та пристрої мають доступ до ресурсів мережі. Моніторинг трафіку. Моніторинг мережевого трафіку дозволяє вчасно виявляти будь-які аномальні активності та потенційні загрози

для безпеки мережі. Оновлення та патчі. Важливо систематично оновлювати програмне забезпечення VPN і патчі для запобігання використанню вразливостей. Фізична безпека серверів. Для захисту від фізичних загроз, таких як крадіжка обладнання, сервери VPN повинні бути знаходитися в безпечних приміщеннях з обмеженим доступом. Ці заходи допомагають забезпечити безпеку та приватність віртуальних приватних мереж. Віртуальні приватні мережі (VPN) – це технологія, яка дозволяє створювати безпечне та приватне з'єднання між різними пристроями через публічну мережу, таку як Інтернет. Основні відомості про віртуальні приватні мережі та завдання забезпечення безпеки мережевого трафіку та мереж можуть включати наступне. Мета використання VPN. Типи VPN. Віддалений доступ (Remote Access VPN). Дозволяє користувачам підключатися до корпоративної мережі з віддалених місць через Інтернет. Сайт-до-сайту (Site-to-Site VPN). З'єднує дві або більше мережі між собою через Інтернет, щоб створити єдину віртуальну мережу. Протоколи та шифрування. Використання шифрування для захисту конфіденційності даних під час передачі через мережу. Популярні протоколи VPN включають OpenVPN, IPsec (Internet Protocol Security), L2TP (Layer 2 Tunneling Protocol), SSTP (Secure Socket Tunneling Protocol), та інші. Аутентифікація та авторизація. Використання методів аутентифікації, таких як паролі, сертифікати, аутентифікація на основі токенів тощо, для перевірки ідентичності користувачів. Авторизація визначає, які ресурси та послуги може використовувати користувач після успішної аутентифікації. Захист від загроз та атак. Виявлення та блокування потенційно шкідливого трафіку. Захист від DDoS (розподілені атаки з обмеженням доступу) та інших мережевих атак. Моніторинг та аудит безпеки. Постійний моніторинг мережі для виявлення потенційних загроз та атак. Проведення аудитів безпеки для перевірки дотримання стандартів безпеки та виявлення можливих уразливостей. Загалом, віртуальні приватні мережі відіграють важливу роль у забезпеченні безпеки мереж та конфіденційності даних у сучасному світі, де з'єднання з Інтернетом стає все більш важливим для роботи, навчання та спілкування.

1.2 Віртуальні приватні мережі VPN

Віртуальні приватні мережі (VPN) мають різноманітні призначення та особливості, які роблять їх важливою технологією для багатьох сфер діяльності. Основні призначення та особливості технології VPN включають. Забезпечення безпеки та конфіденційності даних. Одним з основних призначень VPN є захист даних, які передаються через мережу. Вони шифруються, щоб забезпечити конфіденційність інформації від несанкціонованого доступу. VPN дозволяють користувачам з будь-якої точки з доступом до Інтернету з'єднуватися з приватною мережею, такою як корпоративна мережа. Це дозволяє працювати віддалено з важливими ресурсами та даними компанії. Обхід обмежень географічної блокування. VPN можуть бути використані для отримання доступу до вмісту, який може бути обмежений за географічними межами. Наприклад, користувачі можуть використовувати VPN для доступу до стрімінгових сервісів або веб-сайтів, які обмежують доступ до свого контенту залежно від місця знаходження. Захист від відслідковування та моніторингу. VPN допомагають захистити приватність користувача від стеження інтернет-провайдерів, рекламних компаній та інших сторін, які можуть бажати відстежувати його діяльність в Інтернеті. Захист від вірусів та інших загроз. Використання VPN може допомогти у захисті від шкідливих програм, таких як віруси, шпигунське програмне забезпечення та інші мережеві загрози, шляхом фільтрації трафіку і блокування шкідливих з'єднань. Контроль та управління доступом. Деякі VPN можуть надавати можливість адміністраторам мережі контролювати та управляти доступом користувачів до різних ресурсів та служб мережі. Підвищення пропускної здатності та стабільності з'єднання.

В деяких випадках використання VPN може покращити якість з'єднання, особливо в обстановці, де провайдери Інтернету обмежують або обмежують пропускну здатність для певних видів трафіку. Ці призначення та особливості роблять VPN важливою технологією для захисту та оптимізації мережевої діяльності в сучасному світі. Віртуальні приватні мережі (VPN) мають

різноманітні призначення та особливості, які дозволяють їм вирішувати різні завдання в сфері забезпечення безпеки, приватності та доступу до мережевих ресурсів. Ось деякі з найважливіших призначень та особливостей технології VPN. Забезпечення конфіденційності даних. Однією з основних функцій VPN є шифрування мережевого трафіку, що перешкоджає його перехопленню та читанню третіми особами. Це особливо важливо при використанні непротираного з'єднання, такого як відкриті мережі Wi-Fi в кафе або аеропортах. Забезпечення безпеки з'єднання. VPN дозволяє створювати безпечне з'єднання між вузлами через ненадійну мережу, таку як Інтернет. Використання протоколів шифрування та аутентифікації дозволяє уникнути прослуховування та забезпечити ідентифікацію користувачів. Віддалений доступ. Одним з основних призначень VPN є надання віддаленого доступу до корпоративних ресурсів з будь-якого місця, де є доступ до Інтернету. Це дозволяє співробітникам працювати з важливими даними, не виходячи з дому або подорожуючи. Обход блокування та обмежень. В деяких країнах або мережах блокують доступ до певних веб-сайтів або послуг. VPN дозволяє обходити такі обмеження, забезпечуючи користувачам анонімність та доступ до заблокованих ресурсів. Захист від DDoS-атак. Деякі VPN-провайдери можуть надавати захист від розподілених атак з обмеженням доступу (DDoS). Шифрування та пересилання трафіку через безпечні тунелі допомагають уникнути впливу таких атак на мережеві ресурси. Приватність та анонімність. VPN дозволяють користувачам приховати свою реальну IP-адресу та місцезнаходження, змінюючи їх на IP-адреси серверів VPN. Це забезпечує більшу приватність та анонімність під час використання Інтернету.

Інтеграція з іншими технологіями безпеки. VPN можуть бути інтегровані з іншими технологіями безпеки, такими як файрволи, системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS) тощо, для забезпечення комплексного захисту мережі. Ці призначення та особливості роблять VPN важливим інструментом для забезпечення безпеки, конфіденційності та доступу до мережевих ресурсів у сучасному цифровому світі.

1.3 Критерії, технічні особливості VPN

Віртуальні приватні мережі (VPN) можна класифікувати за різними критеріями, включаючи технічні особливості, способи використання, архітектурні особливості тощо. Нижче подано деякі основні класифікаційні підходи до VPN. Віддалений доступ (Remote Access VPN). Дозволяє користувачам підключатися до центральної мережі з віддалених місць через публічну мережу, таку як Інтернет. Клієнти зазвичай встановлюють VPN-з'єднання з індивідуальних пристроїв до центрального VPN-сервера. Сайт-до-сайту (Site-to-Site VPN). Сполучає дві або більше корпоративні мережі через публічну мережу. Це дозволяє створити безпечне з'єднання між різними мережами. IPsec VPN. Використовує протокол IPsec (Internet Protocol Security) для забезпечення безпеки з'єднання. SSL/TLS VPN. Використовує SSL (Secure Sockets Layer) або його наступник TLS (Transport Layer Security) для створення безпечного з'єднання. OpenVPN. Відкритий протокол VPN, який може працювати на різних платформах та оперативних системах. Індивідуальні VPN. Використовуються одним користувачем або декількома користувачами для забезпечення безпеки та приватності під час використання публічних мереж.

Корпоративні VPN. Використовуються організаціями для забезпечення безпеки, віддаленого доступу та обміну даними між віддаленими філіями та робочими місцями. За методом аутентифікації. VPN з використанням користувача та пароля. Користувачі вказують ім'я користувача та пароль для аутентифікації. VPN з використанням сертифікатів. Користувачі використовують цифрові сертифікати для аутентифікації. За цільовим призначенням. Бізнес-VPN. Використовуються компаніями для забезпечення безпеки мережі та доступу до корпоративних ресурсів. Поточний VPN. Використовуються для обходу обмежень доступу до веб-сайтів або забезпечення анонімності під час використання Інтернету. Ці класифікації допомагають розуміти різні типи VPN та їх використання в різних сценаріях. Вибір певного типу VPN залежить від конкретних потреб організації або

користувача. Мережі VPN рівня 2, також відомі як L2VPN (Layer 2 Virtual Private Networks), забезпечують приватне з’єднання між двома або більше мережами на рівні каналізації даних, тобто на рівні кадрів (фреймів). Основною метою L2VPN є передача даних між мережами без необхідності зміни їхніх IP-адрес або втручання у їхній маршрутизаційний процес. Ось деякі основні види мереж VPN рівня 2. VPWS (Virtual Private Wire Service). VPWS забезпечує приватне з’єднання між двома точками (точка-точка). Використовується для підключення віддалених офісів, філій або дата-центрів. VPLS (Virtual Private LAN Service). VPLS створює віртуальну приватну LAN через публічну мережу. Дозволяє підключати декілька мережевих сегментів так, щоб вони здавалися знаходитися в одній локальній мережі. VPWS та VPLS через MPLS. Ці типи мереж VPN рівня 2 часто будуються використовуючи MPLS (Multiprotocol Label Switching) для пересилання даних. MPLS дозволяє створювати віртуальні тунелі між маршрутизаторами, що спрощує розподіл трафіку і підвищує продуктивність. Основні переваги мереж VPN рівня 2 включають. Прозорість для протоколів верхніх рівнів. Мережа VPN рівня 2 не втручається у протоколи верхніх рівнів, що дозволяє передавати будь-які дані без зміни.

Простота налаштування та управління. Мережі VPN рівня 2 можуть бути відносно простими для налаштування та управління, особливо у порівнянні з мережами VPN рівня 3. Підтримка broadcast і multicast. Деякі реалізації VPN рівня 2 дозволяють передавати broadcast і multicast пакети між віддаленими мережами. Однак важливо враховувати, що мережі VPN рівня 2 можуть бути менш ефективними у розміщенні трафіку та менш гнучкими у порівнянні з мережами VPN рівня 3, які працюють на рівні IP зображено на рисунку 1.1.

Рисунок 1.1 – Мережа VPN [1]

Мережі VPN рівня 3, також відомі як L3VPN (Layer 3 Virtual Private Networks), забезпечують приватне з'єднання між різними мережами на рівні маршрутизації IP. Вони дозволяють передавати дані між різними точками мережі, використовуючи адресування IP та протоколи маршрутизації. Ось деякі основні характеристики мереж VPN рівня 3. Технологія тунелювання. Використання тунельних протоколів, таких як IPsec (для мереж через Інтернет) або MPLS (для приватних мереж), для створення зашифрованого тунелю між вузлами VPN. Тунельна структура дозволяє забезпечити безпеку та конфіденційність даних, переданих через мережу VPN. Використання IP-адрес для ідентифікації та маршрутизації. Кожна мережа VPN рівня 3 має свій власний діапазон IP-адрес, який використовується для ідентифікації вузлів мережі та маршрутизації трафіку. Маршрутизація даних відбувається на основі IP-адрес та інформації про маршрути. Протоколи маршрутизації. Використання протоколів маршрутизації, таких як OSPF (Open Shortest Path First), BGP (Border Gateway Protocol), або RIP (Routing Information Protocol), для встановлення маршрутів між вузлами мережі VPN.

Ці протоколи дозволяють визначити оптимальні шляхи для передачі даних через мережу VPN. Маршрутизація вищого рівня. Мережі VPN рівня 3 дозволяють передавати дані на верхній рівень мережі, такий як рівень застосунків. Це означає, що VPN можуть підтримувати різноманітні застосунки, що вимагають рівня IP для комунікації. Багаторівневий підхід.

Деякі реалізації мереж VPN рівня 3 можуть мати багаторівневу архітектуру, де маршрутизація відбувається на кількох рівнях абстракції, наприклад, мережевий рівень та мережевий рівень застосунків. Приватність мережі та ізоляція. Кожна мережа VPN рівня 3 ізольована від інших мереж, що дозволяє забезпечити приватність та безпеку даних. Мережі VPN рівня 3 є дуже розповсюдженими і дозволяють компаніям побудувати приватні мережі для спільного використання ресурсів та забезпечення безпеки даних. Технологія MPLS VPN (Multiprotocol Label Switching Virtual Private Network) – це метод побудови віртуальних приватних мереж на базі MPLS технології, що дозволяє створювати приватні мережі в середині публічної мережі, такої як Інтернет або WAN (Wide Area Network). Основні характеристики та переваги технології MPLS VPN включають таке. Лейбловане пересилання пакетів. MPLS використовує механізм лейблованого пересилання, де кожен пакет отримує спеціальний міткований лейбл. Цей лейбл використовується для визначення шляху пакету через мережу.

Віртуалізація мережі. MPLS дозволяє віртуалізувати мережевий трафік, що дозволяє створювати приватні логічні мережі незалежно від фізичної мережевої інфраструктури. Сегментація мереж. MPLS VPN дозволяє розділити мережу на окремі сегменти, кожен з яких може мати свої власні правила маршрутизації та безпеки. Приватність та безпека даних. MPLS VPN забезпечує високий рівень приватності та безпеки даних шляхом шифрування даних та використанням механізмів контролю доступу. Керування трафіком. MPLS дозволяє налаштовувати та керувати трафіком в мережі, забезпечуючи оптимальний шлях для передачі даних.

Підтримка різних типів з’єднань. MPLS VPN підтримує різні типи з’єднань, включаючи віддалений доступ (Remote Access), міжфірмові з’єднання (Site-to-Site), а також інтеграцію з різними протоколами VPN. Масштабованість та продуктивність. MPLS VPN дозволяє побудувати великі та високопродуктивні мережі, які можуть ефективно використовуватися для передачі великого обсягу даних. Технологія MPLS VPN є досить поширеною серед підприємств та постачальників послуг інтернету для створення приватних

мереж з високим рівнем безпеки та ефективності передачі даних зображено на рисунку 1.2.

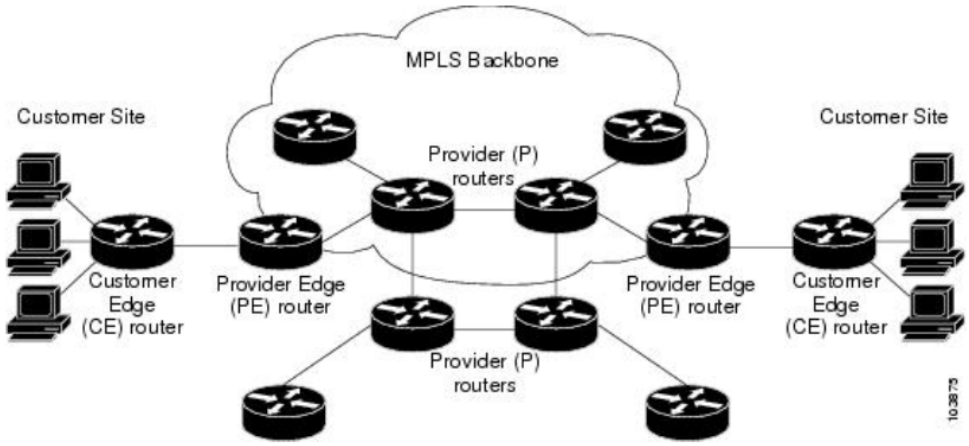

Рисунок 1.2 – Віртуалізація мережі [1]

Технологія MPLS VPN (Multiprotocol Label Switching Virtual Private Network) – це метод побудови віртуальних приватних мереж на базі MPLS технології, що дозволяє створювати приватні мережі в середині публічної мережі, такої як Інтернет або WAN (Wide Area Network). Основні компоненти та особливості технології MPLS VPN включають таке. Лейбловане пересилання пакетів (MPLS). MPLS використовує механізм лейблованого пересилання, де кожен пакет отримує спеціальний міткований лейбл. Цей лейбл використовується для визначення шляху пакету через мережу.

Віртуалізація мережі. MPLS дозволяє віртуалізувати мережевий трафік, що дозволяє створювати приватні логічні мережі незалежно від фізичної мережевої інфраструктури. Тунелювання даних (VPN). MPLS дозволяє створювати віртуальні тунелі між вузлами мережі, що забезпечує приватність та безпеку передачі даних через публічну мережу. Маршрутизація на основі міток (MPLS Label Switching). При використанні MPLS маршрутизація відбувається на основі міток, а не IP-адрес. Це дозволяє швидше пересилати дані та забезпечує більшу гнучкість в управлінні трафіком. Розділення мережі на логічні сегменти (VRF). MPLS VPN використовує VRF (Virtual Routing and Forwarding) для розділення мережі на логічні сегменти, кожен з яких може мати

свою власну таблицю маршрутизації та незалежні VPN. Приватність та безпека даних. MPLS VPN забезпечує високий рівень приватності та безпеки даних шляхом шифрування даних та використанням механізмів контролю доступу. Масштабованість та продуктивність. MPLS VPN дозволяє побудувати великі та високопродуктивні мережі, які можуть ефективно використовуватися для передачі великого обсягу даних. Технологія MPLS VPN є досить поширеною серед підприємств та постачальників послуг інтернету для створення приватних мереж з високим рівнем безпеки та ефективності передачі даних. Вона дозволяє підприємствам побудувати складні мережі з безпекою, які забезпечують необхідні вимоги щодо пропускної здатності, масштабованості та надійності.

У першому розділі визначено, що один із заходів безпеки мережевий трафік і самі мережі є використання віртуального приватного мережі (VPN) з використанням будь-якої комбінації технологій для захисту підключення, тунелювання через незахищену або ненадійну мережу. Забезпечується Основні рекомендації по створенню VPN. Встановлено, що технологія VPN призначена для захисту мережі. взаємодія між територіально розподіленими користувачами може бути реалізовані на різних рівнях моделі OSI і реалізовані в різних реалізаціях, в залежно від необхідної функціональності, розміру мереж і запланованих навантаження на них. Відзначається, що VPN використовують тунелювання за допомогою протоколи IPsec, L2TP, PPTP і SSL, шифрування трафіку для забезпечення конфіденційність даних, автентифікація користувачів і алгоритми забезпечення цілісності даних.

На основі класифікації віртуальних приватних мереж брандмауер на основі апаратного забезпечення і SSL VPN та розглянуто їх особливості. Було досліджено мережі VPN рівня 2 і 3 і надано їх порівняння. Основні відмінності між VPN рівня 3 полягають у визначенні політик і маршрутизація постачальника послуг і потреби клієнтів у спільному використанні інформацію про топологію вашої мережі. Крім того, перемикач CE клієнта повинен бути налаштованим на використання BGP або OSPF для зв’язку з комутатором постачальник послуг. Особливості функціонування технології MPLS VPN і зазначається, що перевагами цієї технології є обслуговування без підключення,

непотрібність тунелів для мережевого шифрування та конфіденційності, централізоване обслуговування, масштабованість, якісна підтримка Сервіс (QoS).

РОЗДІЛ 2
РЕАЛІЗАЦІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Проектування комп'ютерної мережі

Побудова віртуальних приватних мереж (VPN) може бути реалізована за різними способами, залежно від потреб організації, характеристик мережі та бюджетних обмежень. Ось кілька основних варіантів побудови VPN. Site-to-Site

VPN. Цей тип VPN використовується для з’єднання декількох локальних мереж (наприклад, між філіями однієї компанії). VPN-шлюзи на кожній локальній мережі створюють зашифрований тунель через публічну мережу (наприклад, Інтернет). Remote Access VPN. Цей тип VPN дозволяє віддаленим користувачам підключатися до центральної мережі через Інтернет. Користувачі встановлюють VPN-підключення до спеціального VPN-сервера, який надає доступ до ресурсів мережі. Hub-and-Spoke VPN. Цей варіант побудови VPN використовує центральний вузол («хаб»), який обслуговує декілька віддалених вузлів («спіків»). Всі з’єднання між вузлами пройдуть через центральний вузол, що дозволяє керувати трафіком та забезпечує зручний спосіб маршрутизації. Cloud VPN.

У цьому варіанті побудови VPN використовується хмарна інфраструктура для створення віртуальної приватної мережі. Сервіси хмарних провайдерів надають можливість створювати VPN-з’єднання між різними обліковими записами або між хмарними й локальними мережами. Layer 2 VPN. Це віртуальні мережі, які працюють на другому рівні моделі OSI (Data Link Layer), зазвичай використовуються для побудови VPN між різними місцями підприємства. Прикладами є VPLS (Virtual Private LAN Service) і VPWS (Virtual Private Wire Service), які забезпечують віртуальне підключення між вузлами. Software-defined WAN (SD-WAN). SD-WAN поєднує в собі різні типи з’єднань, включаючи VPN, для забезпечення оптимальної мережевої пропускної здатності та ефективності. Ця технологія дозволяє динамічно керувати маршрутизацією трафіку та використовувати найбільш вигідні канали для передачі даних. Ці варіанти надають різноманітні можливості для побудови VPN залежно від потреб вашої організації та характеристик мережі.

2.2 Аутентифікацію та цілісність даних

Протокол безпеки IPsec (IP Security) – це набір протоколів для забезпечення безпеки мережевого зв’язку на рівні мережевого (IP) та надійності передачі даних через публічні мережі, такі як Інтернет. IPsec може

застосовуватися для захисту віртуальних приватних мереж (VPN), а також для забезпечення безпеки точка-точка та кінця-кінця комунікації в мережах. Основні складові протоколу IPsec включають такі протоколи.

AH (Authentication Header). AH забезпечує аутентифікацію та цілісність даних, які передаються між двома кінцями сполучення. AH гарантує, що дані не були змінені під час транспортування через мережу.

ESP (Encapsulating Security Payload). ESP забезпечує аутентифікацію, цілісність та конфіденційність даних. Він шифрує та захищає дані від несанкціонованого доступу.

IKE (Internet Key Exchange). IKE використовується для встановлення безпечного з'єднання між двома кінцями зв'язку. Він встановлює ключі шифрування та аутентифікації, які використовуються для захисту комунікації через IPsec.

IPsec може працювати у різних режимах, включаючи режим тунелювання (для захисту всього IP-пакету) та режим транспортного рівня (для захисту тільки транспортного рівня даних).

Основні переваги протоколу безпеки IPsec включають. Забезпечення конфіденційності, цілісності та аутентифікації даних. Можливість застосування для захисту різних типів трафіку, включаючи IP-телефонію, відео, електронну пошту тощо. Конфігураційна гнучкість та підтримка різних режимів та алгоритмів шифрування. Використання в широкому спектрі мережних пристроїв та платформ. IPsec є одним з найпоширеніших і надійних методів забезпечення безпеки мережевого зв'язку та захисту даних у сучасних мережевих середовищах, що зображено на рисунку 2.1.

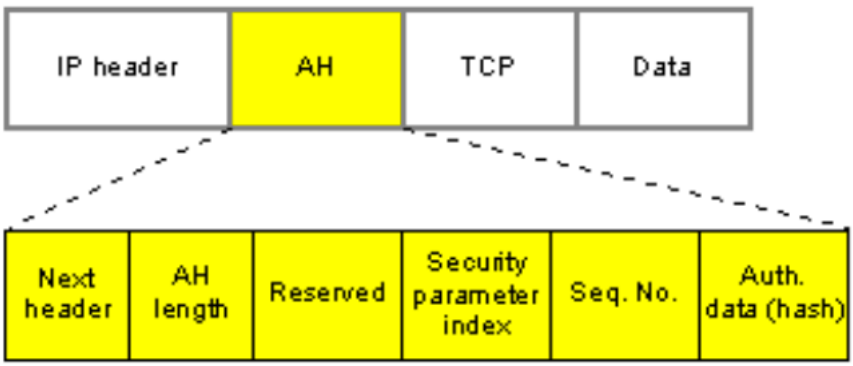

Рисунок 2.1 – Протокол безпеки [2]

Протокол безпеки IPsec (IP Security) – це набір протоколів, призначених для забезпечення конфіденційності, цілісності та автентифікації даних, що передаються через мережі IP. IPsec забезпечує ці безпекові функції на рівні мережевого (Network Layer) та може бути використаний для захисту з'єднань між різними мережами або між окремими пристроями. Основні компоненти та функції IPsec включають наступне. Аутентифікація голови IP (AH – Authentication Header). AH використовується для забезпечення цілісності та аутентичності даних, що передаються через мережу IP. Він додає до IP-пакета заголовок, який містить хеш-значення даних та інформацію про аутентифікацію. Протокол захисту даних (ESP – Encapsulating Security Payload). ESP використовується для шифрування даних, що передаються через мережу IP, забезпечуючи конфіденційність. Він додає до IP-пакета додатковий заголовок, який містить зашифровані дані. Протокол обміну ключами (IKE – Internet Key Exchange). IKE використовується для автоматичного обміну ключами та налаштування параметрів захисту між двома точками, що спілкуються. Він дозволяє встановлювати безпечне з'єднання між вузлами, які взаємодіють через мережу IP. Режими роботи. IPsec підтримує два основних режими роботи. Transport Mode (режим транспорту) та Tunnel Mode (режим тунелювання).

У режимі транспорту лише дані самого IP-пакета захищені, тоді як у режимі тунелювання захищена вся IP-датаграма. Підтримка IPv4 та IPv6. IPsec може застосовуватися як до IPv4, так і до IPv6 мереж. IPsec є широко використовуваним стандартом для захисту мережевого трафіку та забезпечення безпеки в Інтернеті та в корпоративних мережах. Він може бути використаний як для віддаленого доступу до мережі, так і для захисту з'єднань між різними мережами або між окремими пристроями, що зображено на рисунках 2.2-2.3.

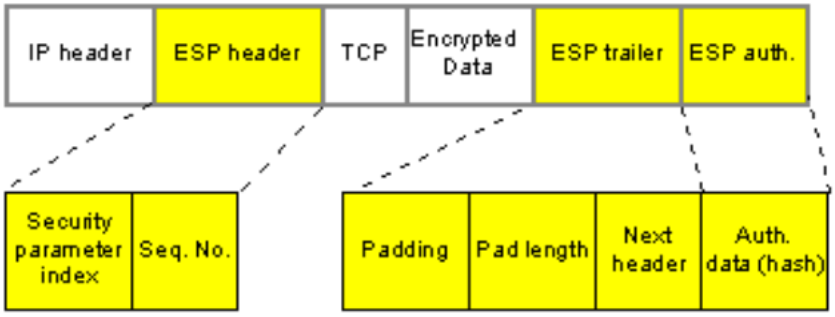

Рисунок 2.2 – Підтримка IPv4 та IPv6 [3]

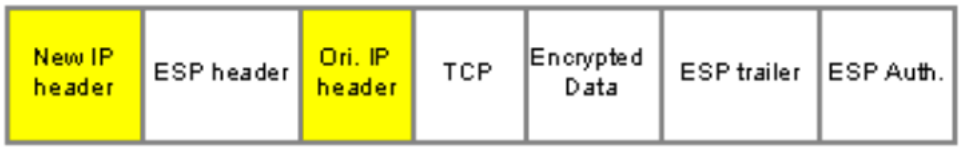

Рисунок 2.3 – Ipsec [4]

Протокол IPsec (Internet Protocol Security) є стандартом безпеки для захисту IP-пакетів в комп'ютерних мережах, забезпечуючи конфіденційність, цілісність та аутентифікацію даних. Він широко використовується для побудови захищених віртуальних приватних мереж (VPN) на базі Інтернету та інших публічних мереж. Основні характеристики та функції протоколу IPsec включають таке. Шифрування даних (Encryption). IPsec може застосовувати криптографічні алгоритми для шифрування даних в IP-пакетах, що забезпечує конфіденційність передачі даних.

Аутентифікація (Authentication). IPsec дозволяє перевіряти автентичність відправника та/або отримувача даних за допомогою різних методів аутентифікації, таких як підписи або обмін ключами. Інтегрітет даних (Data Integrity). IPsec гарантує цілісність даних, забезпечуючи захист від змін або модифікацій під час передачі. Захищений обмін ключами (Secure Key Exchange). IPsec використовує безпечні протоколи для обміну ключами, такі як Internet Key Exchange (IKE), для встановлення безпечних з'єднань між вузлами VPN. Підтримка тунелювання (Tunneling Support). IPsec дозволяє створювати захищені тунелі між вузлами мережі, що забезпечує приватність та безпеку даних під час передачі через неприватні мережі. Підтримка IPv4 та IPv6. IPsec

підтримує як IPv4, так і IPv6, що дозволяє застосовувати його в різних типах мереж та середовищ. Гнучкість конфігурації. IPsec має різні режими роботи, такі як тунельний режим (Tunnel Mode) та режим транспортного рівня (Transport Mode), що дає можливість адаптувати його до конкретних потреб мережі. IPsec використовується як у корпоративних мережах для побудови безпечних VPN, так і в мережах зв'язку, таких як Інтернет, для захисту від несанкціонованого доступу та забезпечення конфіденційності даних, що зображено на рисунку 2.4.

Рисунок 2.4 – Режими роботи Ipsec [4]

Протокол безпеки IPsec (IP Security Protocol) – це набір протоколів для забезпечення безпеки мережевого трафіку на рівні мережевого рівня (рівень IP) в моделі OSI. IPsec використовується для шифрування та аутентифікації даних, що передаються через мережі, забезпечуючи конфіденційність, цілісність та автентифікацію. Основні компоненти IPsec включають.

AH (Authentication Header). AH використовується для забезпечення цілісності та автентифікації даних, які передаються через мережу. Він додає до кожного пакету заголовок, який містить хеш-значення (контрольну суму) та інформацію про аутентифікацію.

ESP (Encapsulating Security Payload). ESP використовується для шифрування даних та захисту їх від прослуховування. Він додає до кожного пакету додатковий заголовок та обгортку, яка містить зашифровані дані.

IKE (Internet Key Exchange). IKE використовується для обміну ключами та налаштування параметрів безпеки між двома кінцями з'єднання. Він дозволяє автоматизувати процес встановлення безпеки із зашифруванням ключів.

IPsec може використовуватися для створення VPN (віртуальних приватних мереж), які забезпечують захищене та конфіденційне з'єднання між двома або більше вузлами через неприватні мережі, такі як Інтернет. Використання IPsec для VPN дозволяє захищати дані, які передаються через мережу, від несанкціонованого доступу та прослуховування. Загалом, IPsec є одним із основних протоколів безпеки для захисту мережевого трафіку, і він широко використовується в різних сценаріях мережевої безпеки, включаючи створення VPN, безпеку з'єднань між вузлами, захист мережевих послуг тощо.

PPTP (Point-to-Point Tunneling Protocol) з GRE (Generic Routing Encapsulation) – це комбінація протоколів, яка використовується для створення віртуальних приватних мереж (VPN) через публічну мережу, таку як Інтернет.

Ось коротка інструкція щодо реалізації PPTP з GRE. Налаштування PPTP-сервера. Встановіть та налаштуйте PPTP-сервер на віддаленому сервері або маршрутизаторі. Настройте аутентифікацію та авторизацію для користувачів, які будуть підключатися до VPN. Встановлення PPTP-клієнта. Встановіть програмне забезпечення або налаштуйте вбудований PPTP-клієнт на пристрої користувача (наприклад, комп'ютері або мобільному пристрої). Налаштуйте параметри підключення до PPTP-сервера, включаючи його IP-адресу або доменне ім'я, інструкції з аутентифікації (якщо необхідно), тощо.

Конфігурація GRE тунелю. Настройте GRE тунель для транспортування трафіку VPN між PPTP-клієнтом і сервером. Використовуйте внутрішні IP-адреси тунелю для передачі даних між кінцями. Проведіть тестування та налагодження. Після налаштування проведіть тестування підключення для перевірки роботи VPN. При необхідності внесіть коригування до налаштувань або параметрів конфігурації для оптимізації роботи VPN. Забезпечення безпеки. Впевніться, що ви використовуєте безпечні методи аутентифікації та шифрування для захисту даних, що передаються через VPN. Регулярно переглядайте налаштування та журнали для виявлення можливих проблем безпеки. Загалом, реалізація PPTP з GRE дозволяє створити простий та зручний спосіб для побудови VPN мережі забезпечення з'єднанням з віддаленими користувачами або між різними офісами, що зображено на рисунку 2.5.

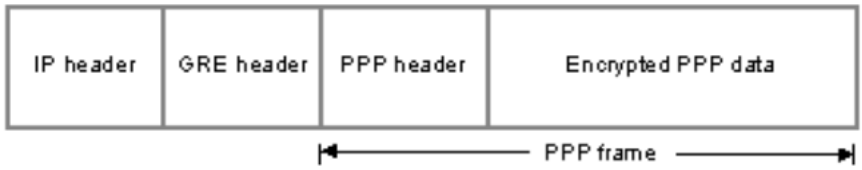

Рисунок 2.5 – Реалізація GRE [5]

Протокол тунелювання L2TP (Layer 2 Tunneling Protocol) – це протокол маршрутизації даних, який часто використовується для створення віртуальних приватних мереж (VPN) або для з'єднання віддалених користувачів з корпоративною мережею. Основна мета L2TP полягає в тому, щоб забезпечити конфіденційність та цілісність даних, переданих через неприватну мережу, таку як Інтернет. Ось деякі основні характеристики протоколу L2TP. Дворівневий протокол. L2TP працює на другому та третьому рівнях моделі OSI (Data Link Layer та Network Layer), що дозволяє передавати дані з відомою адресою і IP-адресою між двома кінцями. Шифрування та аутентифікація. L2TP може бути комбінованим з протоколом шифрування, таким як IPsec, для забезпечення безпеки трафіку. Зазвичай L2TP/IPsec використовується для захисту конфіденційності даних та аутентифікації користувачів.

Підтримка мультимедійних пристроїв. L2TP підтримує передачу мультимедійних даних, що робить його популярним в сферах відеоконференцій та голосового зв'язку. Тунелювання через NAT (Network Address Translation). L2TP може працювати через мережі, що використовують NAT, що робить його ефективним для використання в домашніх мережах та віддалених офісах. Простота налаштування. L2TP є досить простим у налаштуванні та управлінні, що робить його популярним в невеликих та середніх компаніях. Хоча L2TP може бути використаний самостійно, він часто комбінується з іншими протоколами, такими як IPsec, для підвищення рівня безпеки та надійності мережі VPN, що зображено на рисунку 2.6.

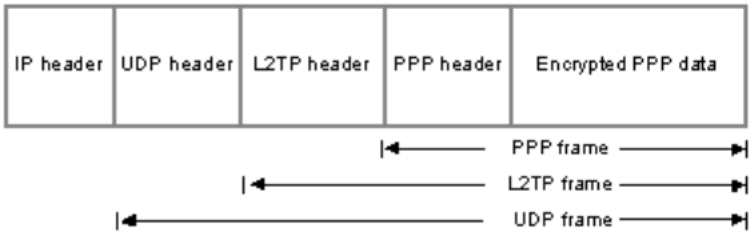

Рисунок 2.6 – Протокол [5]

Протокол SSL/TLS (Secure Sockets Layer / Transport Layer Security) – це криптографічний протокол, який забезпечує безпеку комунікації між двома або більше програмами через комп'ютерну мережу, зазвичай Інтернет. Він використовується для шифрування даних, автентифікації сервера та іноді клієнта, а також для забезпечення цілісності даних. Ось кілька ключових характеристик SSL/TLS. Шифрування даних. SSL/TLS використовує симетричне та асиметричне шифрування для захисту даних, які передаються між клієнтом і сервером. Це забезпечує конфіденційність інформації під час транспортування через мережу. Аутентифікація сервера і (за необхідності) клієнта. SSL/TLS дозволяє перевіряти, що веб-сайт або інший сервер, з яким клієнт спілкується, справді той, за ким він видає себе. Захист від атак типу «man-in-the-middle». Шифрування та аутентифікація, що здійснюються SSL/TLS, роблять труднішим перехоплення або зміна переданих даних третьою стороною. Цифрові сертифікати. SSL/TLS використовує цифрові сертифікати для підтвердження ідентичності сервера та випуску публічного ключа для встановлення безпечного каналу зв'язку.

Підтримка різних версій та алгоритмів. Протокол SSL/TLS має різні версії та підтримує різні криптографічні алгоритми, що дозволяє використовувати найбільш підходящі засоби забезпечення безпеки в конкретних випадках. SSL був розроблений компанією Netscape і став основою для стандарту TLS, який є його розширенням. Використання SSL/TLS широко поширене в Інтернеті, зокрема для забезпечення безпеки веб-переглядачів, електронної пошти, месенджерів та інших онлайн-служб. У цьому розділі пояснюються основні технології тунелювання, визначені принципи їх дії, призначення та сфера

застосування у віртуальн приватні мережі. Проаналізовано основні реалізації VPN. Remote Доступ – для зв’язку між територіально розподіленими філіями та Site-to-Site – для віддаленого доступу користувачів до ресурсів корпоративної мережі робочі місця. Це показують детальні структури фрейму, розглянуті в цьому розділі підвищена безпека при передачі даних у VPN без істотних додаткових навантаження обладнання досягається додаванням спец заголовки кадрів. У цьому випадку перетворення даних у кадрі не відбувається.

Особливу увагу приділено протоколу IPsec як основі роботи захищені з’єднання, принцип обміну ключами, аутентифікація та режими працювати. Через підвищення вимог до безпеки та цілісності даних, застосовуються не тільки до великих корпоративних мереж, а й до підключень звичайні користувачі, впровадження VPN з обов’язковим використанням протоколи безпеки стають критичними.

РОЗДІЛ 3
СТВОРЕННЯ МЕРЕЖЕВОГО ЗВ’ЯЗКУ ТА ВИКОНАННЯ ЕКСПЕРИМЕНТІВ

3.1 Технології для експериментального стенду

Створення експериментального стенду може бути дуже корисним для тестування нових технологій, розробки програмного забезпечення або вивчення принципів мереж та систем. Ось деякі загальні вимоги до обладнання для створення експериментального стенду.

Комп’ютери та сервери. Мінімум два комп’ютери або сервери для створення мережевого зв’язку та виконання експериментів. Комп’ютери

повинні мати достатньо потужний процесор, оперативну пам’ять і сховище для виконання необхідних операцій.

Мережеве обладнання. Мережеві комутатори або маршрутизатори для побудови мережевої інфраструктури. Можливо, знадобиться використання мережевого обладнання з підтримкою різних протоколів маршрутизації та комутації для вивчення їх роботи.

Віртуальне обладнання. Віртуальні машини або контейнери для створення віртуальних середовищ для тестування та розробки. Використання віртуального обладнання дозволяє ефективно використовувати ресурси та швидко створювати різні конфігурації середовищ.

Мультимедійне обладнання. Веб-камери, мікрофони та інші пристрої для тестування мультимедійних застосунків або систем зі спрощеними умовами. Монітори та периферійні пристрої. Монітори для відображення робочого середовища та результатів експериментів. Клавіатури, миші та інші периферійні пристрої для керування та взаємодії з комп’ютерами. Інструменти для моніторингу та аналізу. Програмне забезпечення для моніторингу мережевого трафіку, аналізу роботи протоколів та виявлення можливих проблем. Інструменти для відлагодження та аналізу коду для розробки програмного забезпечення. Додаткове обладнання. Відповідно до конкретних завдань стенду, може знадобитися додаткове обладнання, таке як датчики, актуатори, мережеві сенсори тощо схема стенду зображена на рисунку 3.1-3.2 та таблиці 3.1.

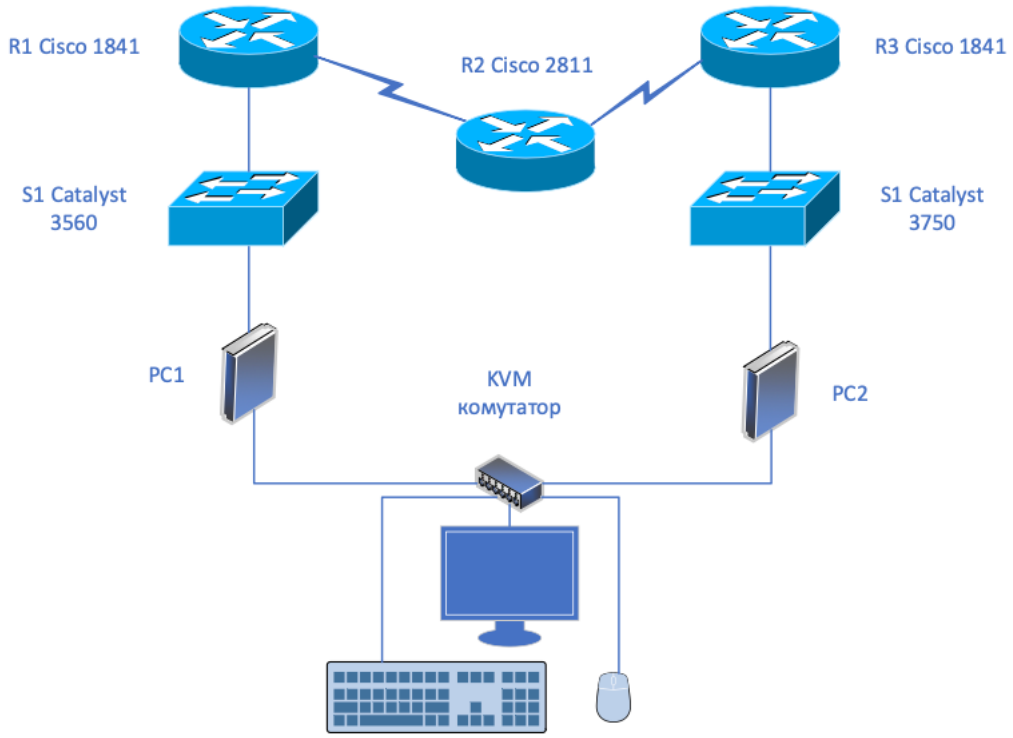

Рисунок 3.1 – Зображення експерименту

Таблиця 3.1 – Характеристика маршрутизатора

(1, 5, 13-16)	Слот розширення для модулів WIC, VWIC (data only для Cisco 1841), або HWIC	(7)	USB порти
(2)	Кріплення для замка Kensington Security Slot	(9)	Порт для керування Aux port
(3, 8)	Порти Fast Ethernet ports та LEDs	(10)	Вимикач живлення
(4)	Консольний порт	(11)	Гніздо живлення
(6)	Слот для карти пам'яті CompactFlash memory card slot	(12)	Слот розширення для модулів NM

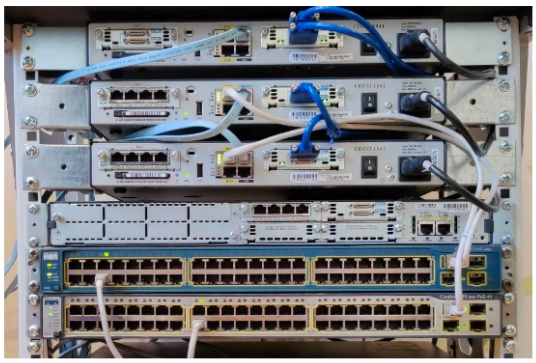

Рисунок 3.2 – Стенд монтаж [5]

3.2 Операційна система

Вибір операційної системи для вашого експериментального стенду залежить від кількох факторів, таких як цілі експериментів, потреби у підтримці програмного забезпечення, ресурси обладнання та особисті уподобання. Ось деякі основні операційні системи та їх характеристики, які можуть бути корисними при виборі. Windows є популярною операційною системою, яка має велику базу користувачів та підтримку багатьох програм та додатків. Вона є досить простою у використанні та має добре розроблену графічну інтерфейс. Windows підтримує багато видів обладнання, що робить його відмінним вибором для різноманітних експериментів. Linux – це вільна та відкрита операційна система з великим вибором дистрибутивів, таких як Ubuntu, Fedora, CentOS тощо. Вона має потужні можливості конфігурації та володіє широким спектром програмного забезпечення та інструментів для розробки та тестування. Linux відомий своєю стабільністю, ефективністю та можливістю роботи на різних платформах обладнання. macOS є операційною системою, розробленою компанією Apple, і вона використовується на комп’ютерах MacBook і iMac. Вона має інтуїтивний інтерфейс та великий вибір програмного забезпечення, а також вбудованих інструментів розробки, таких як Xcode. FreeBSD – це операційна система з відкритим кодом, яка використовується для серверів та вбудованих систем. Вона відома своєю стабільністю та безпекою, що робить її популярним вибором для великих проектів та експериментів з мережами. Іноді можуть бути використані інші

операційні системи, такі як Solaris, OpenBSD, NetBSD тощо, залежно від специфічних потреб та вимог експерименту. При виборі операційної системи важливо враховувати ваші уподобання, навички в роботі з певними ОС, а також конкретні потреби вашого експерименту, Advanced IP Services у ієрархії версій IOS зображено на рисунку 3.3, версії IOS та мінімальний обсяг пам’яті, що потребується подається в таблиці 3.2.

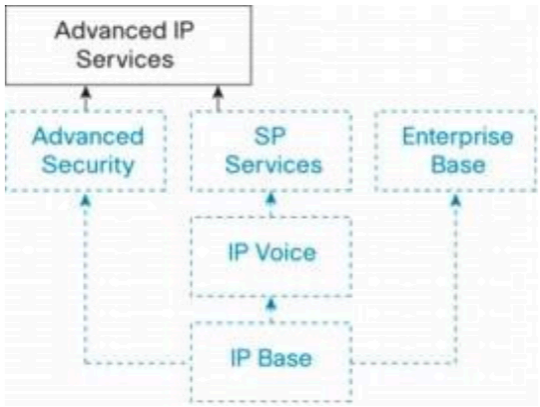

Рисунок 3.3 – Advanced IP Services

Таблиця 3.2 – Характеристики для IOS

Advanced IP Services для:	Назва образу ОС	Мінімальний обсяг FLASH-пам’яті	Мінімальний обсяг DRAM-пам’яті
Cisco 1841	c1841-advipservicesk9-mz.151-4.M12a.bin	64MB	192MB
Cisco 2811	c2800nm-advipservicesk9-mz.151-4.M12a.bin	128MB	512MB

Вибір операційної системи для експериментального стенду залежить від багатьох факторів, таких як тип досліджень, наявність обладнання, доступність програмного забезпечення та особисті вподобання. Ось деякі популярні операційні системи, які можуть бути використані для створення експериментального стенду. Windows є широко використовуваною

операційною системою, яка має велику базу програмного забезпечення, включаючи багато спеціалізованих інструментів для розробки та тестування. Вона може бути корисною для експериментів, що включають розробку програмного забезпечення для Windows або тестування веб-сайтів у браузерах Windows.

Linux є відкритою операційною системою з великою кількістю дистрибутивів, таких як Ubuntu, Debian, Fedora, CentOS тощо. Вона часто використовується для розробки та тестування програмного забезпечення, а також для створення мережевих середовищ, серверів та інших систем.

macOS є операційною системою, яка широко використовується в галузі розробки програмного забезпечення та дизайну. Вона може бути корисною для експериментів, пов’язаних з розробкою для платформи macOS або інтеграцією з продуктами Apple.

FreeBSD – це Unix-подібна операційна система, яка часто використовується для створення серверів та мережевих пристроїв. Вона може бути корисною для експериментів, пов’язаних з мережевою безпекою, розробкою серверного програмного забезпечення та тестуванням мережевих протоколів. Залежно від специфіки ваших експериментів, ви також можете розглядати інші операційні системи, такі як OpenBSD, Solaris, Chrome OS тощо. При виборі операційної системи важливо враховувати ваші потреби, знання та доступні ресурси, а також підтримку програмного забезпечення, яке ви збираєтеся використовувати на вашому стенді.

3.3 Створення та налаштування тунелю GRE

Налаштування Site-to-Site VPN на обладнанні Cisco з використанням технології тунелювання IPsec вимагає кількох кроків. Давайте розглянемо основні етапи налаштування. Створення і налаштування тунелю IPsec. Налаштуйте параметри IPsec, такі як протоколи шифрування, хеш-функції та параметри ключів на обох кінцях VPN (локальному та віддаленому). Створіть

transform-set (набір трансформацій), який визначає параметри шифрування та аутентифікації.

Створіть crypto map, що використовує transform-set та визначає правила обробки IP-пакетів, які потрібно зашифрувати та надіслати через тунель IPsec.

Створення та налаштування тунелю GRE (Generic Routing Encapsulation). Настройте тунель GRE для передачі мережевих пакетів між локальним та віддаленим мережевими інтерфейсами.

Настройка маршрутизації для тунелю IPsec та GRE. Визначте маршрути для трафіку, який має бути надісланий через тунель IPsec. Визначте маршрути для трафіку, який має бути надісланий через тунель GRE. Перевірка та тестування з'єднання VPN. Перевірте стан тунелю IPsec та GRE на обох сторонах з'єднання.

Перевірте можливість передачі даних через VPN, включаючи тестування з'єднання між вузлами мережі. Моніторинг та управління VPN. Налаштуйте моніторинг для стеження за станом тунелю IPsec та GRE, а також для виявлення будь-яких проблем. Встановіть необхідні механізми управління, наприклад, для перезапуску тунелю в разі відмови або для зміни конфігурації VPN.

FreeBSD – це Unix-подібна операційна система, яка часто використовується для створення серверів та мережевих пристроїв. Вона може бути корисною для експериментів, пов'язаних з мережевою безпекою, розробкою серверного програмного забезпечення та тестуванням мережевих протоколів.

Налаштування VPN на обладнанні Cisco може бути складним і вимагає досвіду з мережевою адміністрацією та знань технології IPsec. Використовуйте офіційну документацію Cisco та рекомендації виробника для налаштування VPN згідно з вашими потребами та умовами мережі, яка зображена на рисунку 3.6, IP-адресація в таблиці 3.3 та рисунку 3.4.

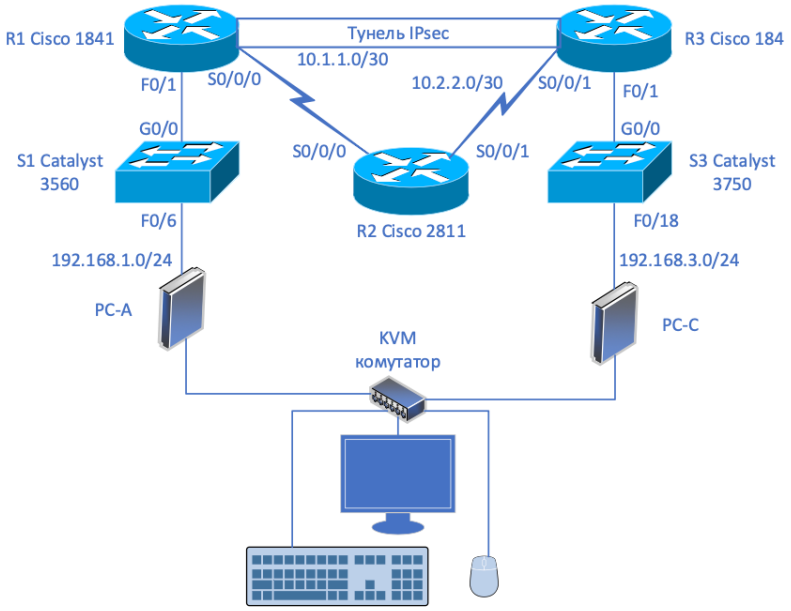

Рисунок 3.4 – Технологія IPsec

Таблиця 3.3 – Характеристика мережі

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням	Порт комутатора
R1	F0/1	192.168.1.1	255.255.255.0	N/A	S1 G0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	F0/1	192.168.3.1	255.255.255.0	N/A	S3 G0/0
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Налаштування Site-to-Site VPN з використанням технології тунелювання IPsec на обладнанні фірми Cisco може бути здійснене за допомогою пристроїв Cisco ASA (Adaptive Security Appliance) або маршрутизаторів Cisco IOS. Ось загальна процедура налаштування. Налаштуйте IPsec на обох маршрутизаторах чи пристроях ASA. Це включає в себе визначення параметрів захисту, таких як алгоритми шифрування, аутентифікації та обмін ключами. Налаштуйте IPsec transform-set, crypto ACL (Access Control List) та IKE policy. Створення тунелю IPsec VPN. Визначте параметри тунелю VPN, такі як IP-адреси тунельних

інтерфейсів, тунельні групи та інші налаштування. Налаштування IKE (Internet Key Exchange). Встановіть параметри IKE, такі як режими обміну ключами, методи аутентифікації та ключі обміну. Визначення тунельних адрес для маршрутизації. Вкажіть, які мережі будуть маршрутизовані через IPsec тунель, і додайте відповідні маршрути. Налаштування мережевих політик та безпеки. Встановіть правила безпеки для трафіку, який проходить через IPsec тунель, за допомогою ACL або функцій мережевої політики ASA. Перевірка та тестування. Перевірте статус тунелю IPsec на обох кінцях. Відправте тестовий трафік через VPN для перевірки з'єднання та функціональності. Це загальний опис процесу. Точні кроки та налаштування можуть відрізнятися в залежності від конкретних моделей пристроїв Cisco та версій програмного забезпечення. Для отримання детальних інструкцій рекомендується використовувати документацію Cisco або консультуватися з фахівцями з мережевої безпеки.

3.4 Створення груп користувачів та налаштування аутентифікації

Для налаштування Remote Access VPN з використанням технології тунелювання IPsec на обладнанні фірми Cisco (наприклад, Cisco ASA), ви можете використовувати технологію Cisco AnyConnect VPN. Ось загальна процедура налаштування. Встановлення Cisco AnyConnect VPN сервера. Встановіть і налаштуйте Cisco AnyConnect VPN сервер на маршрутизаторі Cisco ASA. Створення груп користувачів та налаштування аутентифікації. Створіть групи користувачів для Remote Access VPN та визначте методи аутентифікації (наприклад, локальна база даних, RADIUS, LDAP тощо). Конфігурація IPsec VPN профілю. Налаштування підключень AnyConnect. Встановіть параметри підключення AnyConnect VPN, такі як IP-адреси пулів для надання клієнтам, параметри шифрування, обмін ключами та інші налаштування безпеки. Створення маршрутів та політик безпеки. Визначте маршрути та політики безпеки для трафіку, який пройде через VPN тунель. Налаштування сертифікатів SSL / TLS (опціонально). Якщо використовувати сертифікати SSL / TLS для аутентифікації сервера, встановіть та налаштуйте

сертифікати на маршрутизаторі Cisco ASA. Проведення тестування та перевірка використання захищених протоколів аутентифікації та шифрування показано на рисунку 3.5-3.12 та таблиці 3.4.

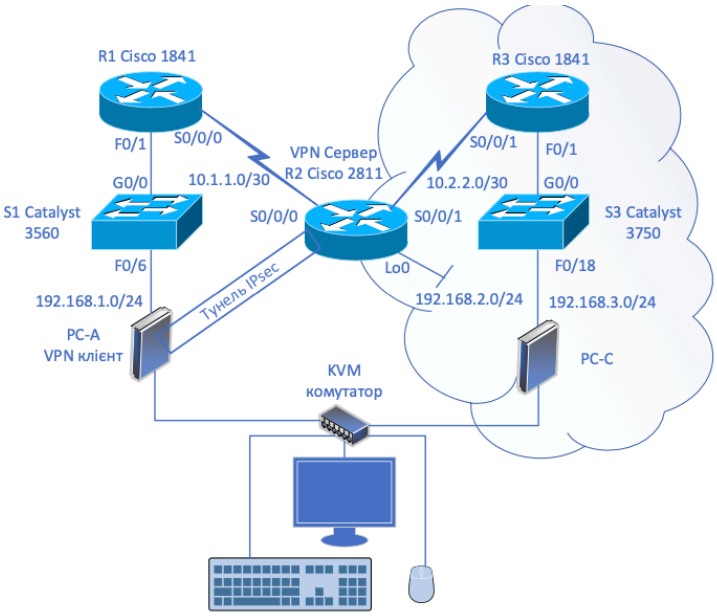

Рисунок 3.5 – Зображення мережі

Таблиця 3.4 – Характеристики мережі

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням	Порт комутатора
R1	F0/1	192.168.1.1	255.255.255.0	N/A	S1 G0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	Loopback 0	192.168.2.1	255.255.255.0	N/A	N/A
R3	F0/1	192.168.3.1	255.255.255.0	N/A	S3 G0/0
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Рисунок 3.6 – Регулювання мережі

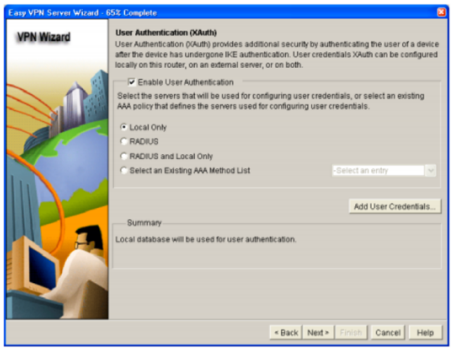

Рисунок 3.7 – Вхід в базу

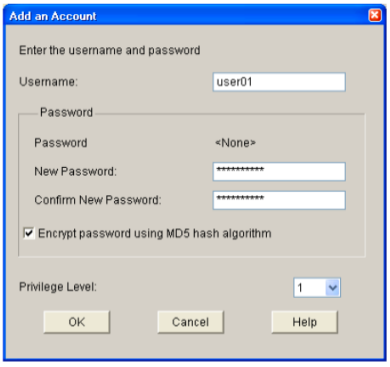

Рисунок 3.8 – Налаштування облікового запису

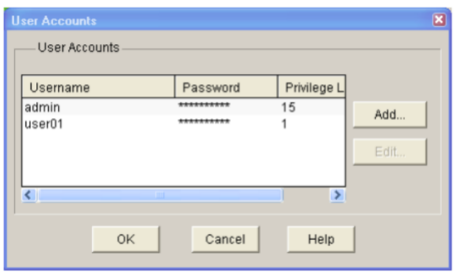

Рисунок 3.9 – Контроль

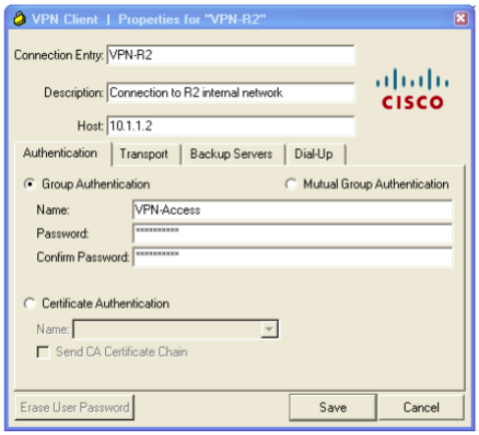

Рисунок 3.10 – Вхід в систему

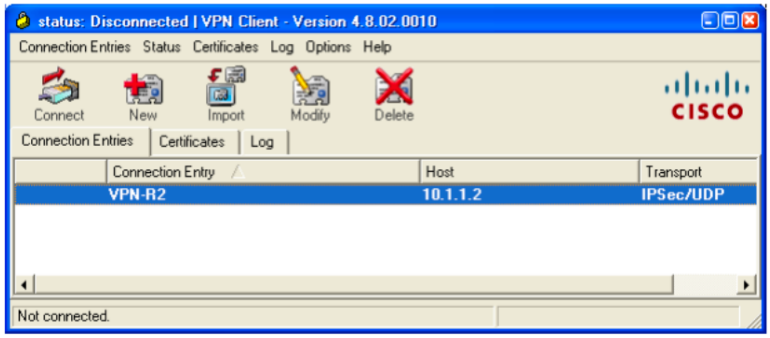

Рисунок 3.11 – Об’єднання мережі

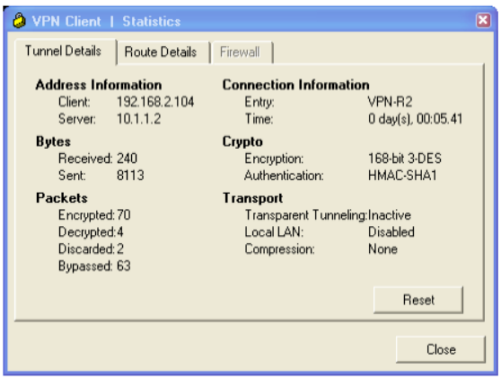

Рисунок 3.12 – Характеристики системи

У сучасному світі, де тісно інтегровані різні інформаційні технології не тільки у великих корпоративних мережах, а й у повсякденному житті звичайних користувачів, впровадження віртуальних приватних мереж з обов’язковим використанням протоколи безпеки стають критичними. Треба захищати буквально всі сфери людської діяльності, починаючи з персональних даних

простих користувачів до мереж великих корпорацій і сервісів провайдери с. Дедалі частіше збитки від різних кіберзагроз є навіть серйозними кошторис. Таким чином, у цій роботі аналізуються заходи безпеки мережевий трафік, пояснюється призначення та особливості технології віртуальні приватні мережі (VPN), необхідність тунелювання, шифрування, автентифікація та цілісність даних. Встановлено, що технологія VPN призначена для захисту мережі. взаємодія між територіально розподіленими користувачами може бути реалізовані на різних рівнях моделі OSI і реалізовані в різних реалізаціях, в залежно від необхідної функціональності, розміру мереж і запланованих навантаження на них. Відзначається, що VPN використовують тунелювання за допомогою протоколи IPsec, L2TP, PPTP і SSL, шифрування трафіку для забезпечення конфіденційність даних, автентифікація користувачів і алгоритми забезпечення цілісності даних. На основі класифікації віртуальних приватних мереж брандмауер на основі апаратного забезпечення і SSL VPN та розглянуто їх особливості. Було досліджено мережі VPN рівня 2 і 3 і надано їх порівняння риса. Основні відмінності між VPN рівня 3 полягають у визначенні політик і маршрутизація постачальника послуг і потреби клієнтів у спільному використанні інформацію про топологію вашої мережі. Також клієнтський комутатор повинен бути налаштованим на використання BGP або OSPF для зв'язку з комутатором постачальник послуг.

Особливості функціонування технології MPLS VPN і зазначається, що перевагами цієї технології є обслуговування без підключення, непотрібність тунелів для мережевого шифрування та конфіденційності, централізоване обслуговування, масштабованість, якісна підтримка Сервіс (QoS). Досліджено основні технології тунелювання та визначено їх принципи робота, призначення та застосування у віртуальних приватних мережах. Проаналізовано основні реалізації VPN. Віддалений доступ – для зв'язку між географічно розподілені філії та Site-to-Site – для доступу користувачів ресурси корпоративної мережі з віддалених робочих станцій. Особливу увагу приділено протоколу IPsec як основі роботи. захищені з'єднання, принцип обміну ключами, аутентифікація та режими працювати. Провідним виробником активного обладнання для

Інтернету вже є. Кілька десятиліть залишилася корпорація Cisco Systems, яка не тільки існує виробник обладнання, а також розробник міжнародних стандартів у цій галузі телекомунікації Тому особлива увага в цій роботі приділялася реалізації віртуальні приватні мережі на основі рішень Cisco.

Освоєння синтаксису командного рядка Cisco IOS дозволив нам налаштувати та перевірити роботу Site-to-Site і VPN віддаленого доступу – дві базові реалізації цієї технології. Безпека передачі даних може бути досягнута різними методами, в т.ч в залежності від критичності даних і технічних можливостей самих мереж Найкращим рішенням є те, яке одночасно забезпечує тунелювання, шифрування, автентифікація та цілісність даних Основою для створення безпечних мереж VPN є використання протоколу безпеки IPsec у побудованих тунелях, оскільки це принцип створення та обміну ключами, аутентифікація існує вже давно стандарт для мереж з критичним трафіком і дозволяє розвивати більше поглиблені параметри для створення безпечних тунелів, таких як VTI VPN, DMVPN і Flex VPN.

ВИСНОВКИ

Розроблено детальний план мережі, що включає вибір необхідного обладнання Cisco (маршрутизатори, комутатори, точки доступу тощо) – для забезпечення стабільного та швидкого з’єднання;

Встановлено та налаштовано мережеве обладнання відповідно до проекту. Впровадження комп’ютерної мережі на основі обладнання Cisco дозволило значно оптимізувати бізнес-процеси салону краси, що сприяло підвищенню продуктивності персоналу та якості обслуговування клієнтів.

Використано сучасні технології захисту від несанкціонованого доступу, вірусів та інших загроз, що включає міжмережеві екрани (firewalls), системи виявлення і запобігання вторгненням (IDS/IPS). Автоматизовано рутинні завдання, таких як запис клієнтів, управління графіками та облік матеріалів, дозволяє зменшити час на виконання цих задач та мінімізувати можливі помилки.

Налаштовані системи резервного копіювання даних та планів аварійного відновлення для забезпечення безперервної роботи бізнесу. Обладнання Cisco забезпечує високу надійність і стабільність роботи мережі, що є критично важливим для безперервної роботи салону.

Впровадити системи управління записами, управління персоналом та обліку матеріалів для зменшення ручної роботи і мінімізації людських помилок;

Використання розширених засобів кібербезпеки, таких як міжмережеві екрани (firewalls), VPN, системи виявлення і запобігання вторгненням (IDS/IPS), дозволяє ефективно захистити дані клієнтів і внутрішню інформацію від несанкціонованого доступу та кіберзагроз.

Забезпечена безшовної інтеграція з системами точок продажу (POS) для оптимізації фінансових транзакцій та управління інвентарем. Мережеве рішення на базі Cisco легко масштабується, що дозволяє без суттєвих додаткових витрат розширювати мережу при збільшенні кількості клієнтів або відкритті нових філій.

Забезпечено швидкий та надійний доступ до онлайн-сервісів, таких як бронювання послуг та програми лояльності, підвищує зручність для клієнтів і сприяє збільшенню їхньої задоволеності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Text Summarization using NLTK: TF-IDF Algorithm. URL: https://itmaster.biz.ua/electronics/arduino/arduino-ide.html (дата звернення: 15.02.2024).

2. Brief Introduction to Neural Networks. URL: https://www.hamlab.net/mcu/training/proteus.html (дата звернення: 15.02.2024).

3. A Complete Guide To Artificial Neural Network In Machine Learning: https://radio-detaly.com/oscilografi-vidi-ta-tipi (дата звернення: 10.02.2024).

4. How neural networks work. URL: https://geekmatic.in.ua/ua/arduino_osnovyi_programmirovaniya (дата звернення: 15.02.2024).

5. Understanding Activation Functions in Neural Networks. URL: https://arduinka.biz.ua/blok-zhivlennya-9v-1a-p297c75.html (дата звернення: 20.02.2024).

6. Neural networks versus Logistic regression for 30 days all-cause readmission prediction. URL: https://en.wikipedia.org/wiki/ATmega328 (дата звернення: 20.02.2024).

7. Deep Learning for NLP. URL: https://vencon.ua/ua/articles/kak-vybrat-batarejku-ili-akkumulyator-vybiraem-batarejki-akkumulyatornye-i-obychnye (дата звернення: 20.02.2024).

8. Word2vec Made Easy. URL : https://www.hwlibre.com/uk/tft/ (дата звернення: 20.02.2024).

9. How is GloVe different from word2vec? URL: https://electronica.in.ua/ua/p1630184399-ostsilograf-dso-shell.html (дата звернення: 20.02.2024).

10. What are the advantages and disadvantages of Word2vec and GloVe? URL : https://uk.fmuser.net/content/?11010.html (дата звернення: 20.02.2024).

11. How is GloVe different from word2vec?. URL : https://www.guru99.com/uk/analog-vs-digital.html (дата звернення: 20.02.2024).

12. Distributed Representations of Words and Phrases and their Compositionality. Головна | Elib LNTU. URL : https://elib.lntu.edu.ua/sites/default/files/elib_upload/ipv/page10.html (дата звернення: 20.02.2024).

13. Word2Vec Tutorial Part I: The Skip-Gram Model. URL : https://radio-shop.com.ua/uk/osnovni-parametry-ostsylohrafiv (дата звернення: 20.02.2024).

14. Electronics for Beginners: A Practical Introduction to Schematics, Circuits, and Microcontrollers. O'Reilly Online Learning. URL: https://www.oreilly.com/library/view/electronics-for-beginners/9781484259795/ (date of access: 20.02.2024).

15. ABCs of Electronics: An Easy Guide to Electronics Engineering. O'Reilly Online Learning. URL: https://www.oreilly.com/library/view/abcs-of-electronics/9798868801341/ (date of access: 20.02.2024).

16. Circuit Design and Simulation Quick Start Guide: Create Schematics and Layout Electronic Components. URL: https://www.oreilly.com/library/view/circuit-design-and/9781484295823/ (date of access: 20.02.2024).

17. PCB Design for Absolute Beginners: Layout Printed Circuit Boards in a Web Browser. URL: https://www.oreilly.com/library/view/pcb-design-for/9781484280409/ (date of access: 20.02.2024).